symantec™

Understanding and Countering Emerging Threats to Critical Information: providing actionable data to state and local entities

John McCumber

Chief Strategist, Public Sector

Agenda

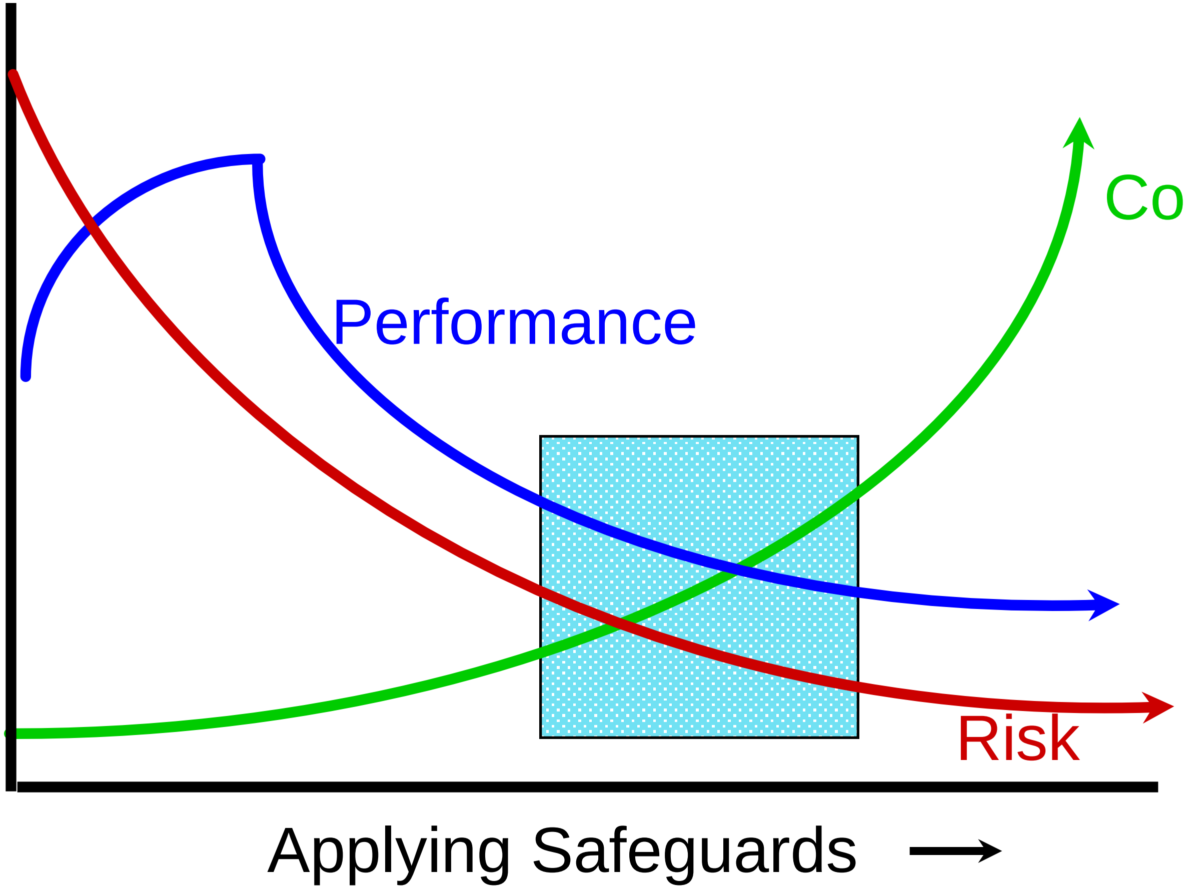
1 Understanding Threat within Risk Management

2 The Role of the Federal Government

3 ISTR XV – Threat Landscape

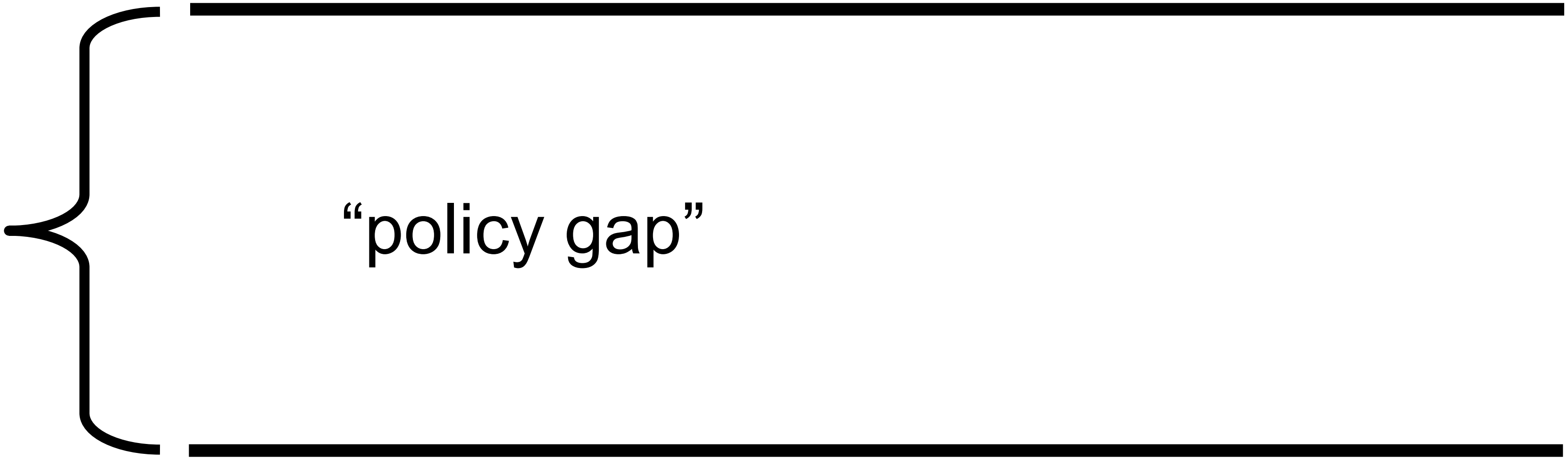
4 Defending Against Threats

Empirical Objective



Filling the Policy Gap

Policy – what you can define/mandate



“policy gap”

Technology tools – what you can enforce

Essential Elements of Risk

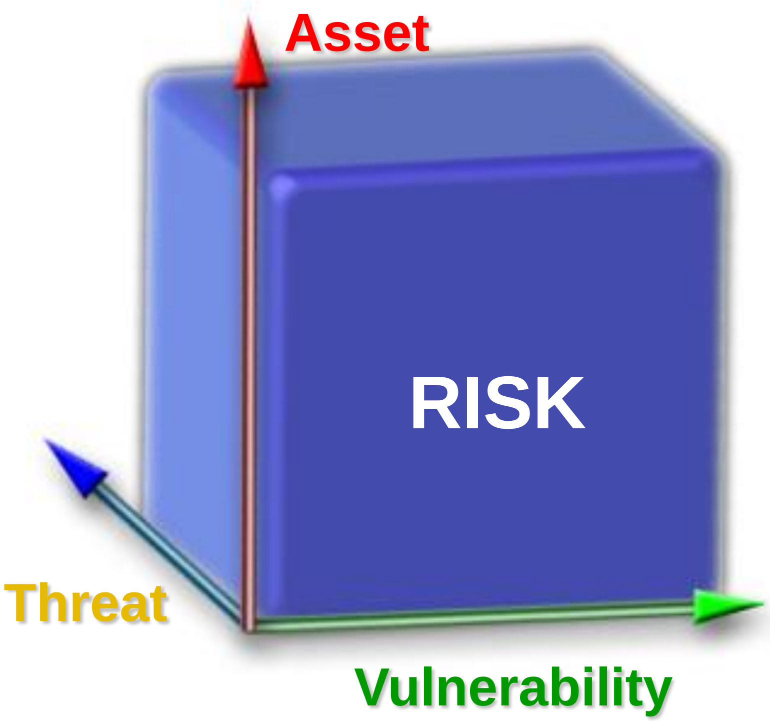
- Threats
- Assets
- Vulnerabilities
- Safeguards
  - Products
  - Procedures
  - People

The Risk Element Relationship

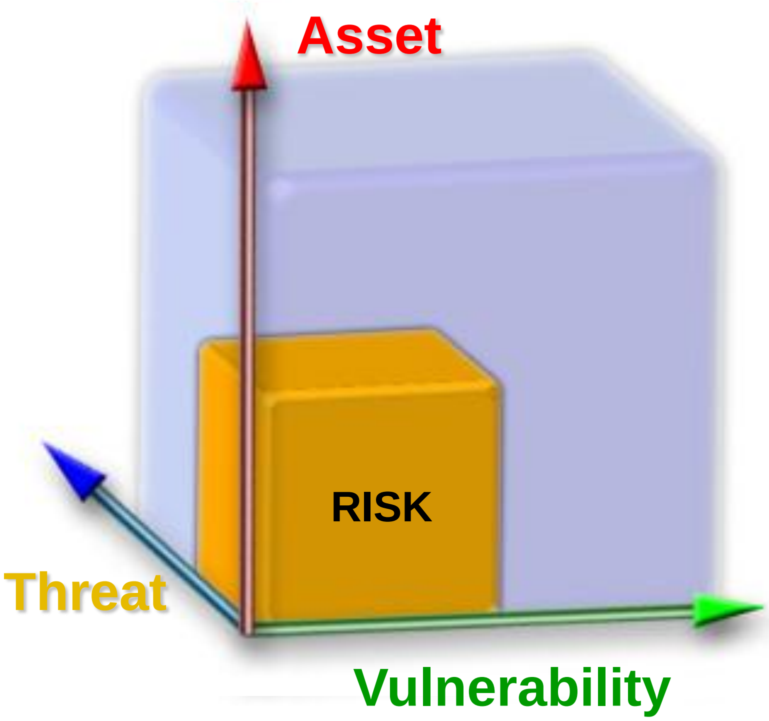
1: $$T \times V \times A = R_b$$

2: $$\frac{T \times V \times A}{S} = R_r$$

Mitigating Risk



Baseline Risk



Residual Risk after Safeguards Applied

The Role of the Federal Government

Fed’s “Should Do” List

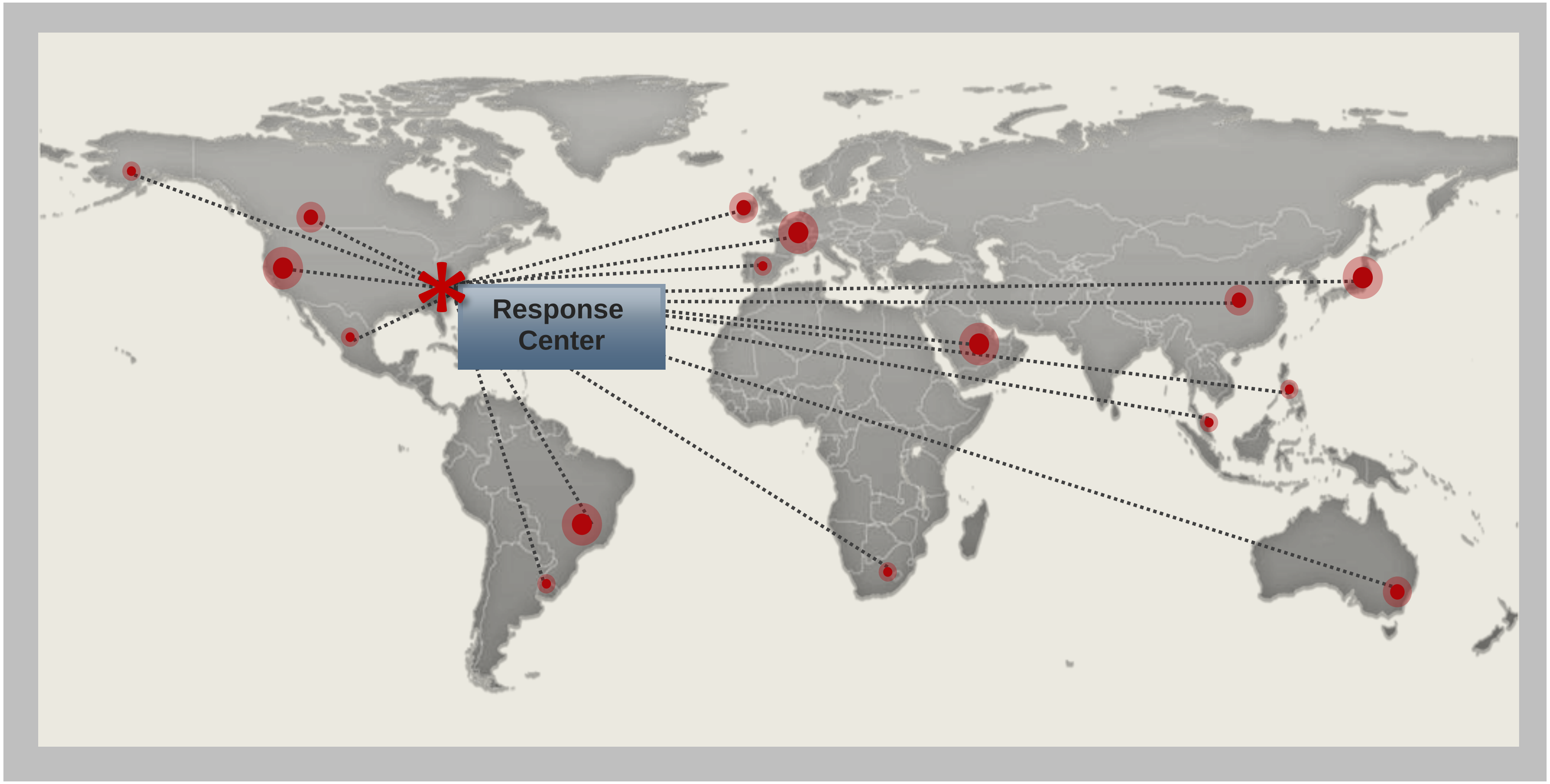
- Define the process of security, rather than an end-state
  - Risk management framework
  - On-going updates
  - Training and support
- Provide process tools
  - Codified and automated toolset
  - Maintain and manage the process
  - Training and more training
- Obtain and distribute required data as available
  - Vulnerabilities
  - Threats –both industry-provided and government specific

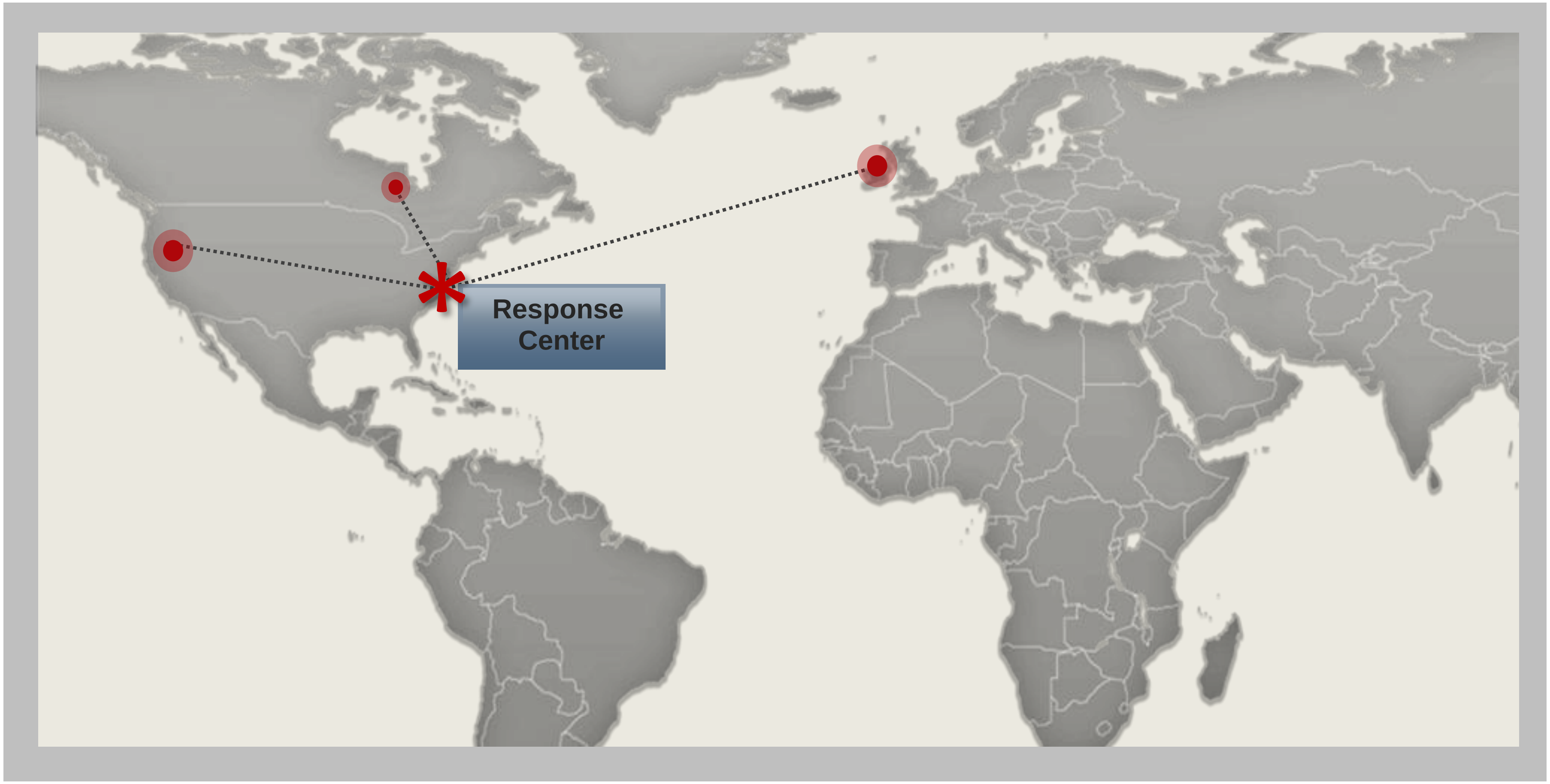
Fed’s “Should Not Do” List

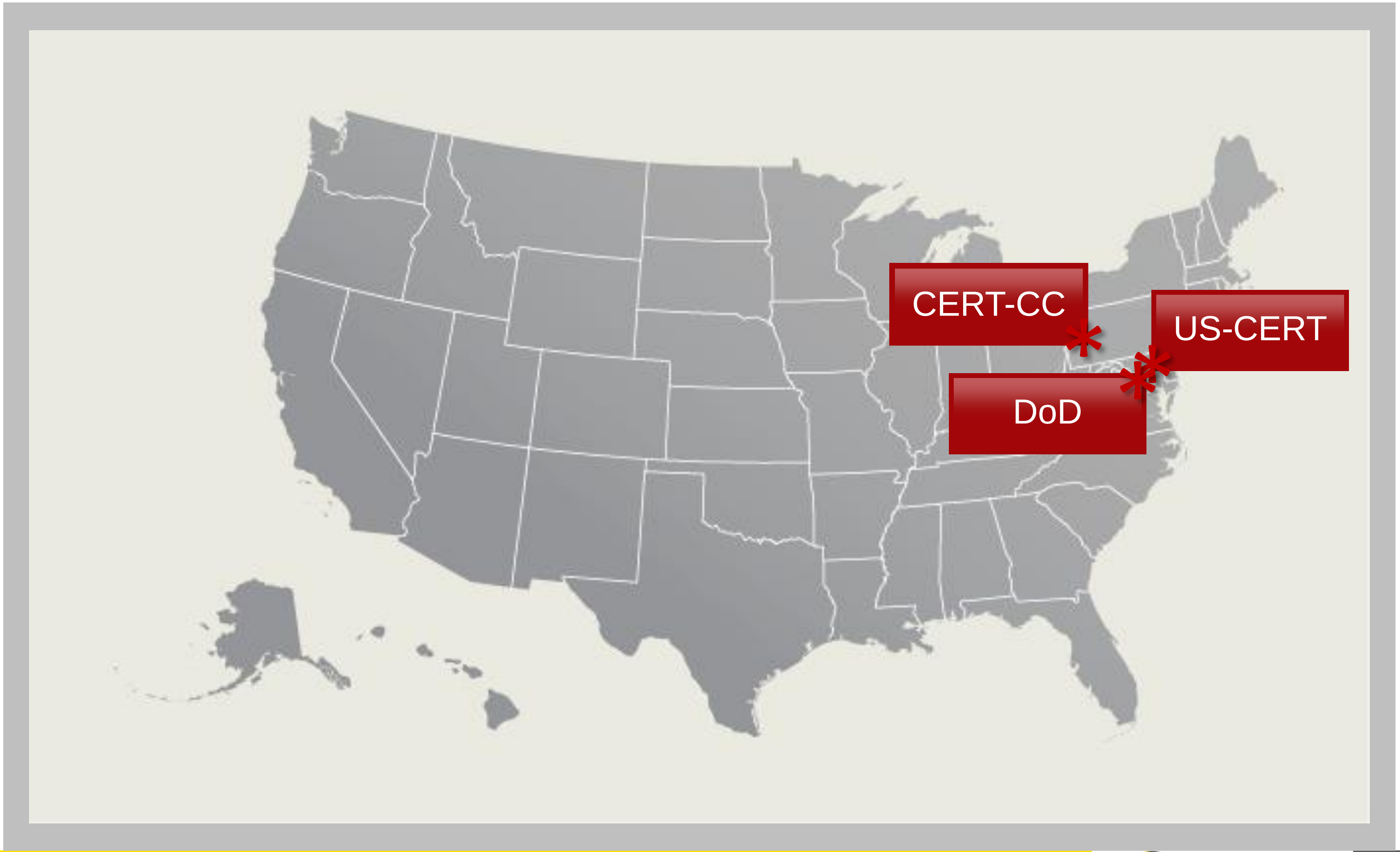
- Dictate a security end-state
  - One-size-fits-none
  - Require product evaluations that, when combined into a functioning system, are meaningless
  - Maintain unenforceable mandates and “approved” architectures
- Build and maintain what they can rent or buy
  - Vulnerability data
  - Threat data
  - Process tools
    - COTS
    - GOTS
- Over-classify

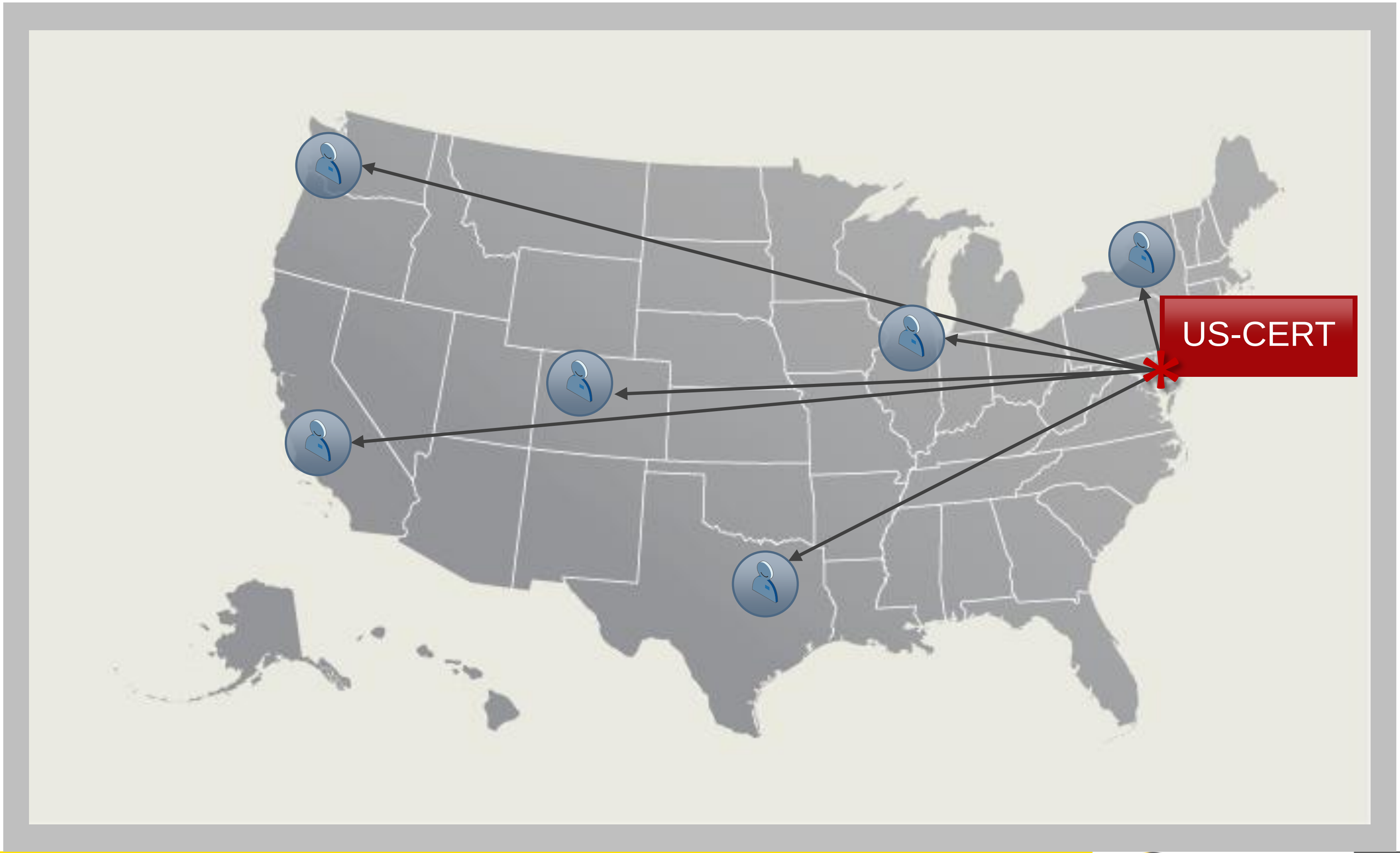
Certification of Personnel

- Who is a cyber security professional?
  - CISSP?
  - NSA Cert holder?
  - Technical cert holder?
  - B.S. or M.S.
  - All of the above
  - None of the above
- Government versus private industry
  - Cross fertilization has always been good
  - Scholarships
    - Government
    - Private colleges and universities

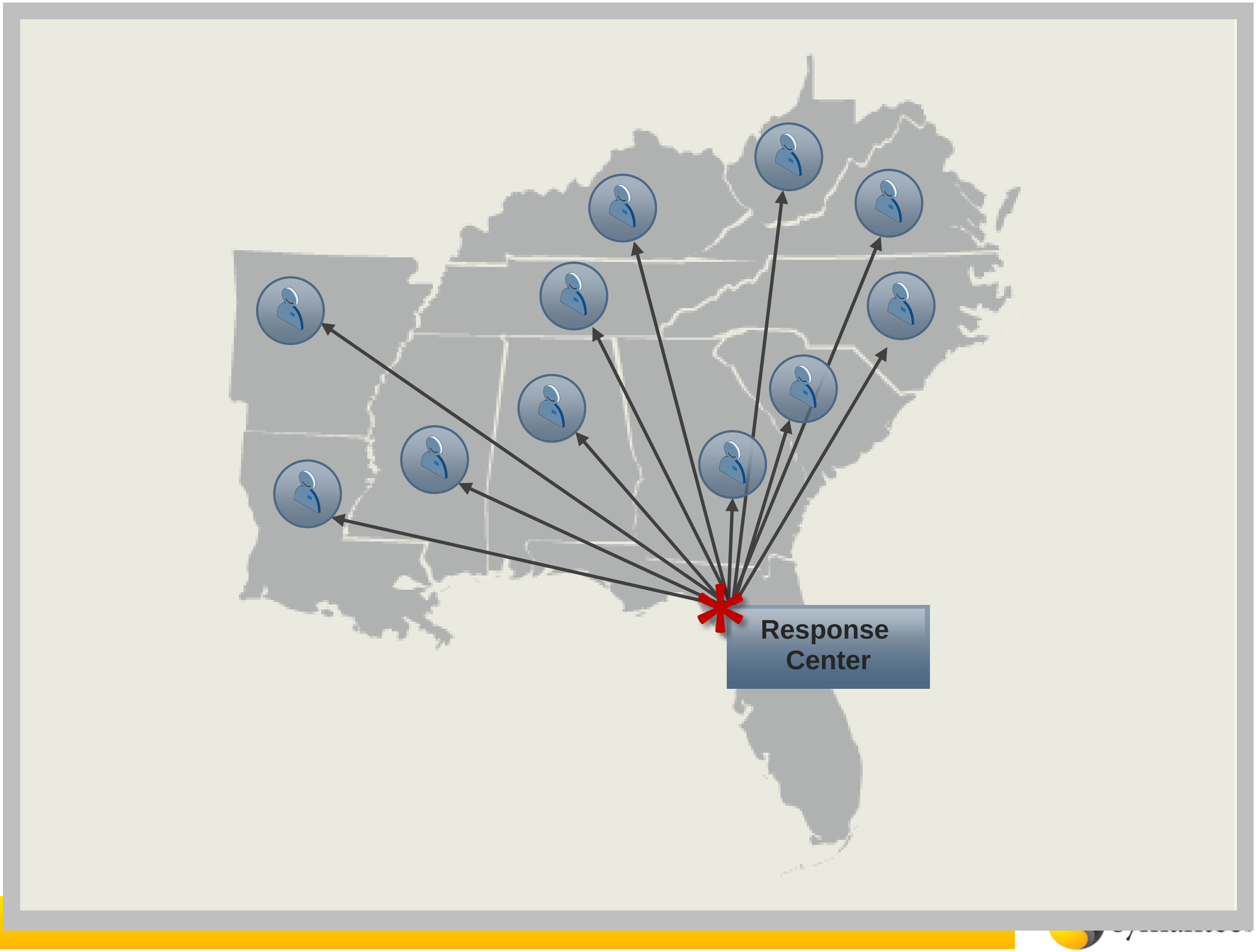

Response
Center


Response Center

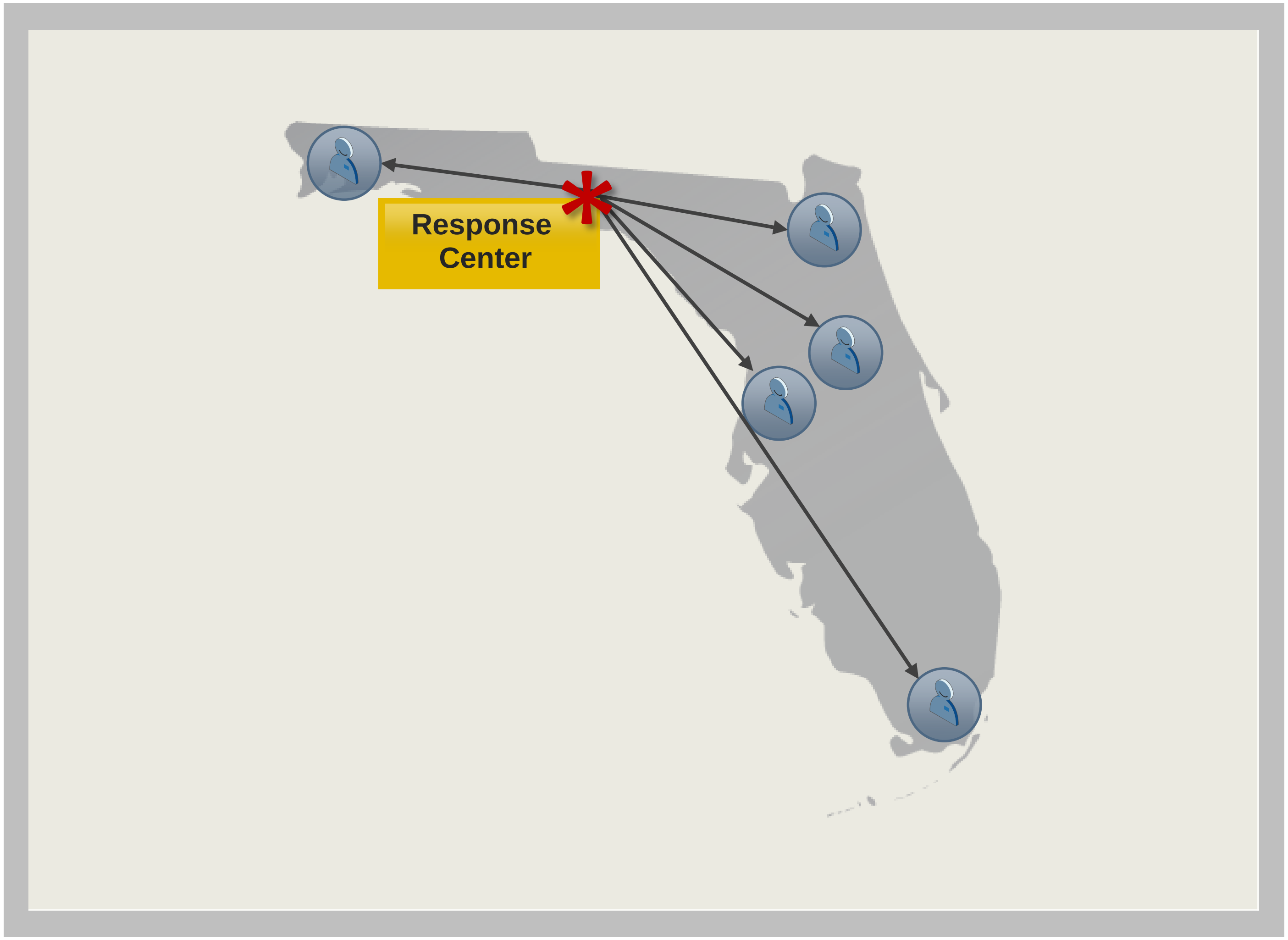

CERT-CC
US-CERT
DoD



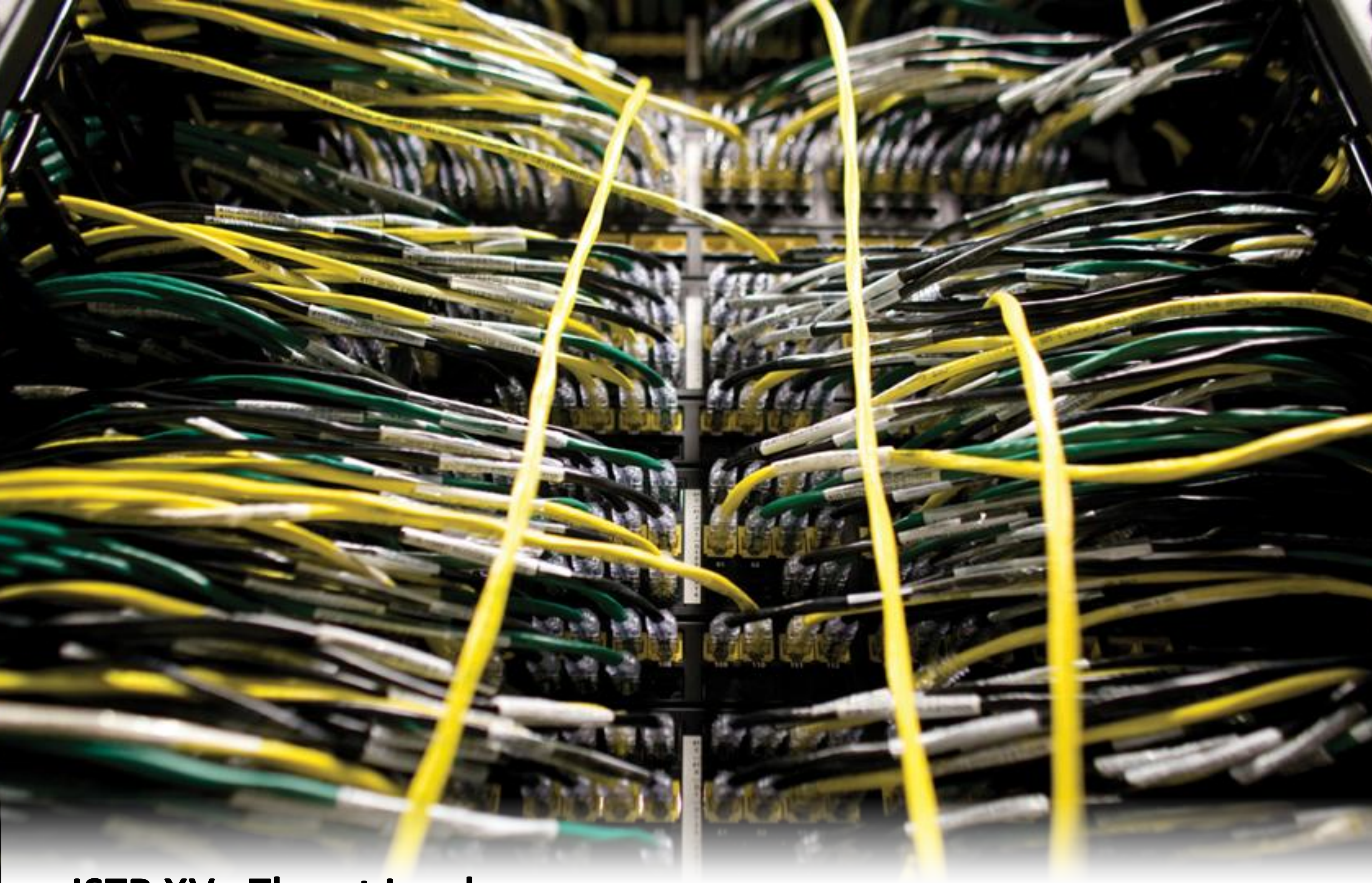
US-CERT



Response Center



Response
Center



ISTR XV: Threat Landscape

Symantec Security

Global Intelligence, Analysis, Protection

Relevancy

Global Expertise

More researchers

Comprehensive data sources

More virus samples analyzed

Extensive customer support

Accuracy

In-depth Analysis

Signatures: AV,AS,IPS,GEB, SPAM, White lists

DeepSight Database

IT Policies and Controls

Rigorous False Positive Testing

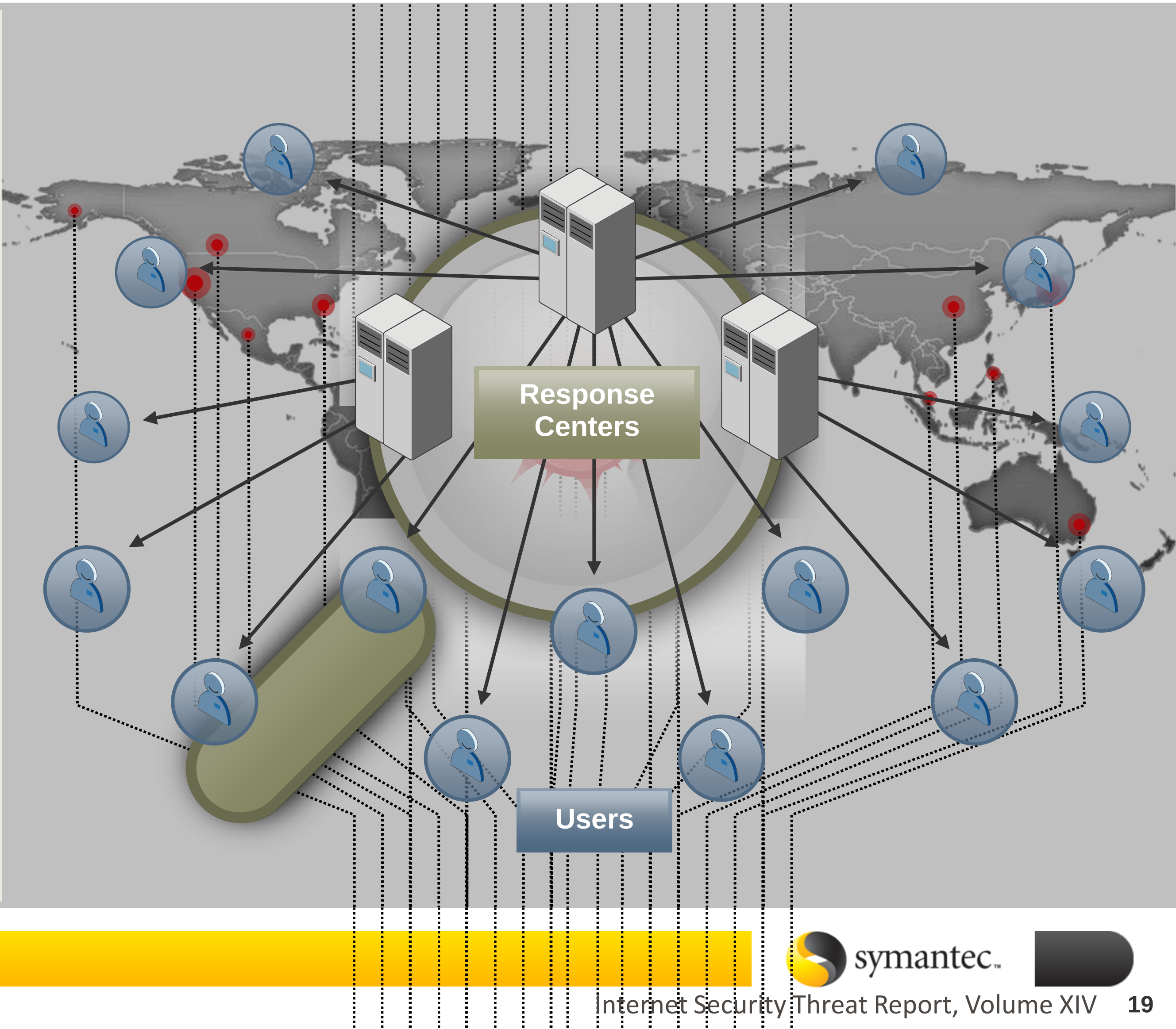
Protection

Automated Updates

Fast & Accurate

Variety of Distribution Methods

Relevant Information

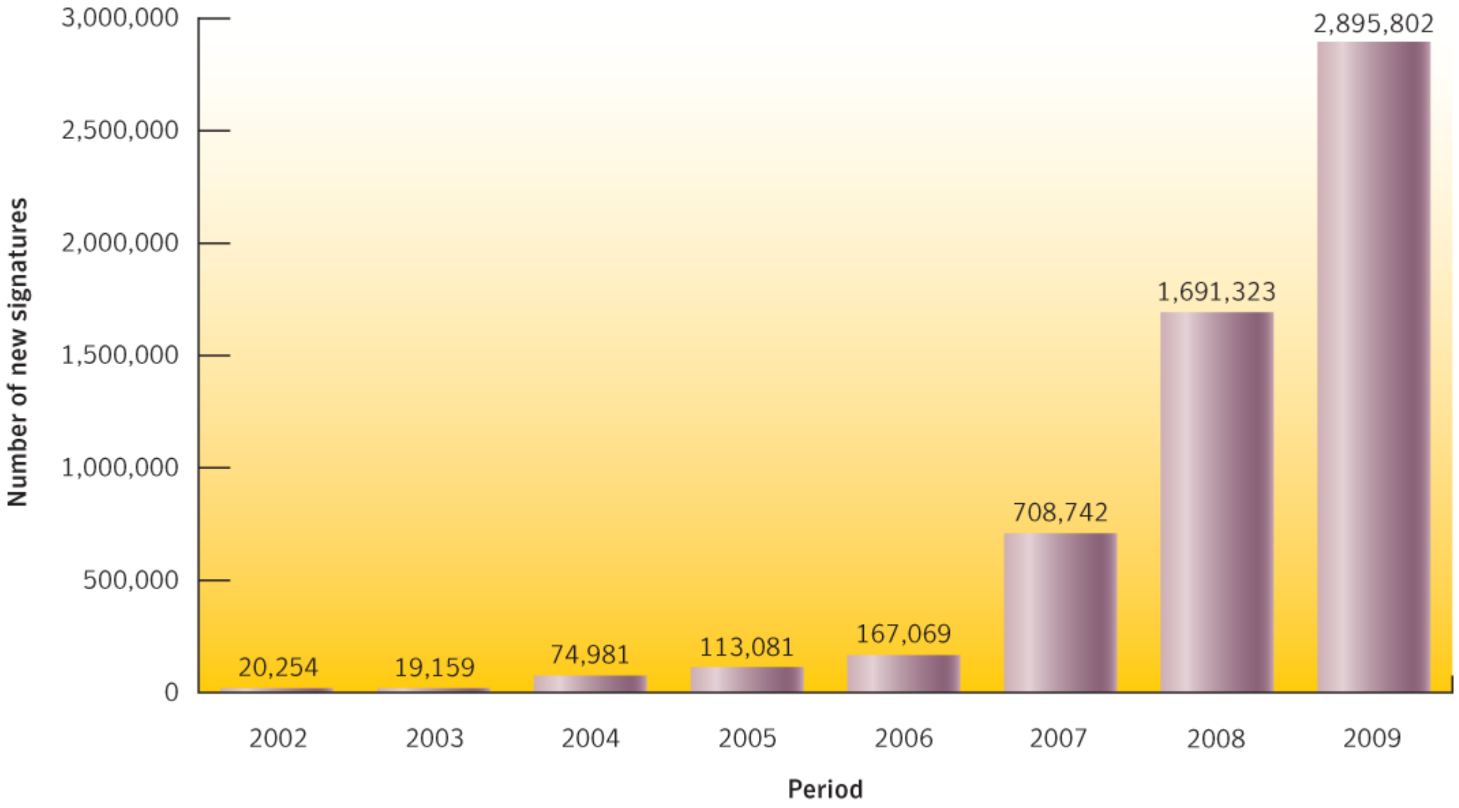


Key Trends in Threat Landscape

- Targeted attacks focus on enterprises
- Web-based attacks still plague users
- Novices enabled with attack kits make theft easy
- Underground economy unaffected by global economy
- Malicious activity takes root in emerging countries

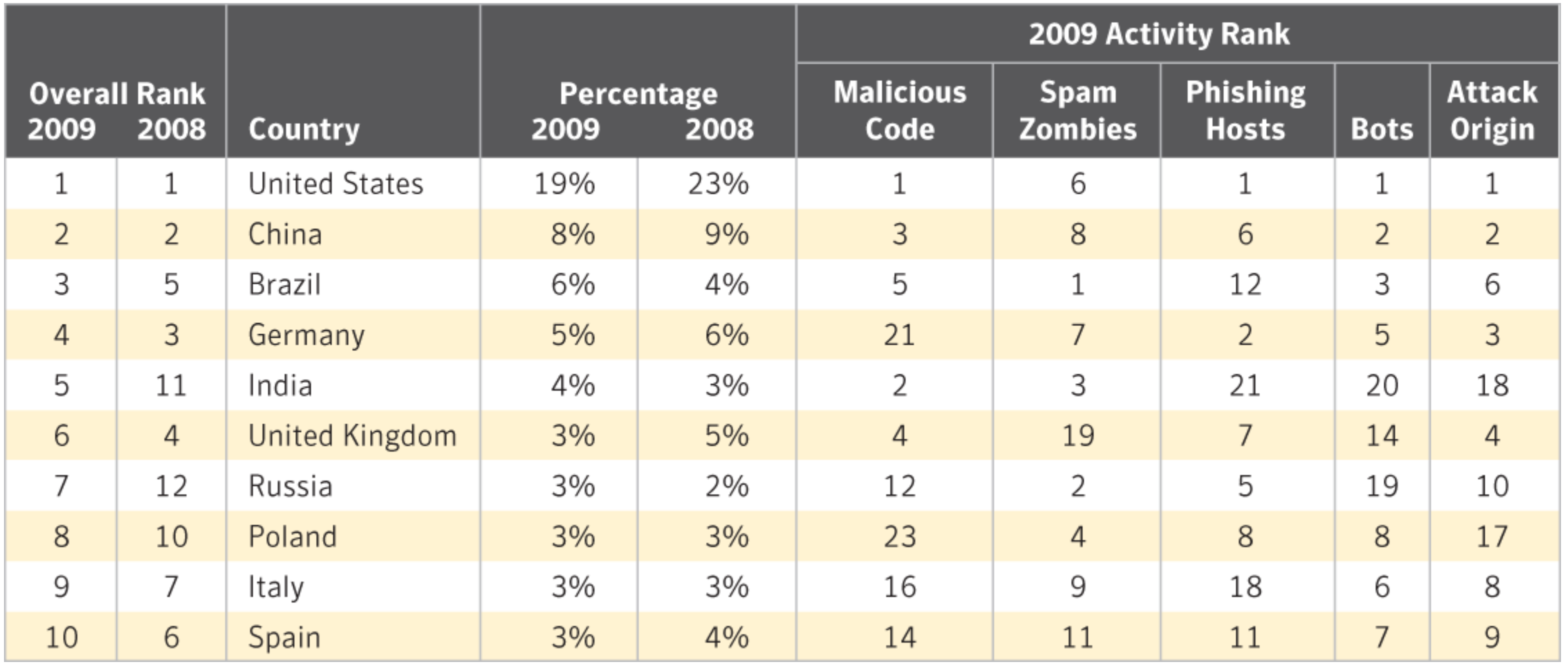
Malicious Code Trends: New Malicious Code Signatures

- A 71% increase over 2008
- 51% of all signatures were created in 2009



Threat Landscape: Malicious Activity in Emerging Countries

- Brazil, India and Poland all saw growth in malicious activity
- Bandwidth attracts cyber criminals
- Cybercriminals move to emerging markets to grow market share

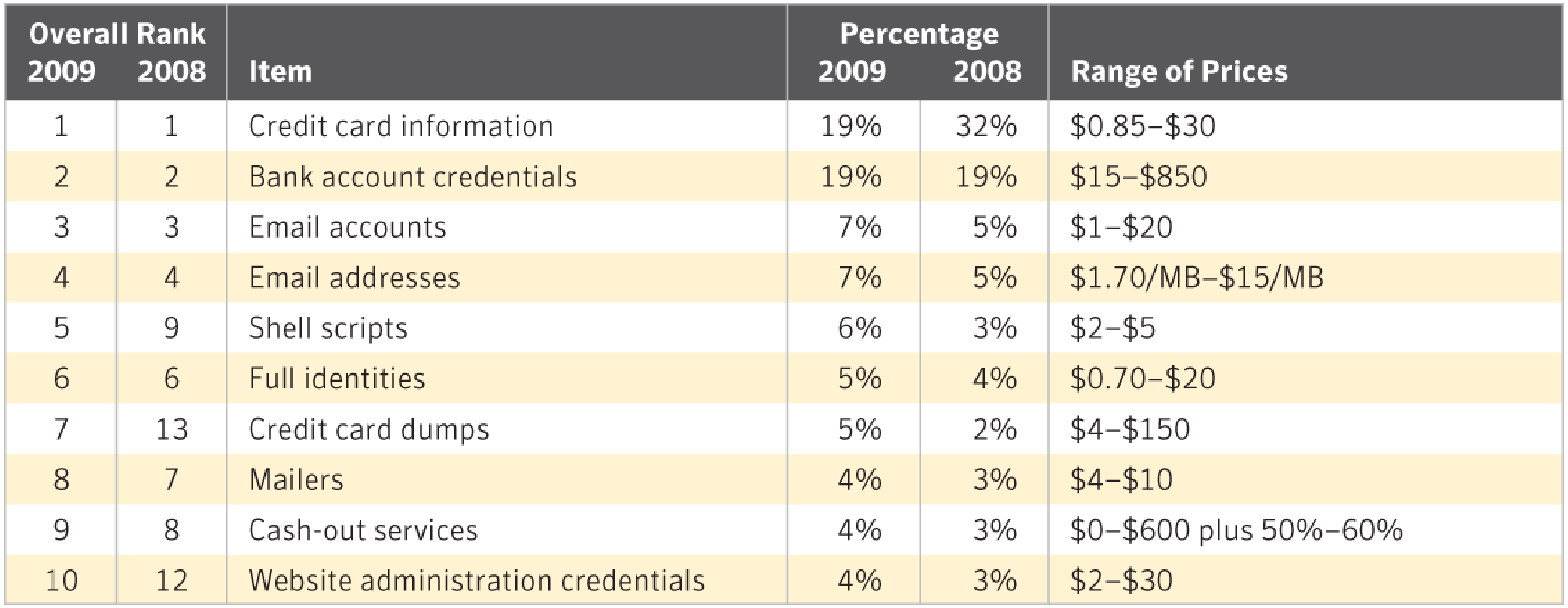


Overall Rank			Percentage		2009 Activity Rank				
2009	2008	Country	2009	2008	Malicious Code	Spam Zombies	Phishing Hosts	Bots	Attack Origin
1	1	United States	19%	23%	1	6	1	1	1
2	2	China	8%	9%	3	8	6	2	2
3	5	Brazil	6%	4%	5	1	12	3	6
4	3	Germany	5%	6%	21	7	2	5	3
5	11	India	4%	3%	2	3	21	20	18
6	4	United Kingdom	3%	5%	4	19	7	14	4
7	12	Russia	3%	2%	12	2	5	19	10
8	10	Poland	3%	3%	23	4	8	8	17
9	7	Italy	3%	3%	16	9	18	6	8
10	6	Spain	3%	4%	14	11	11	7	9

Malicious Activity by Country

Threat Landscape: Underground Economy Still Strong

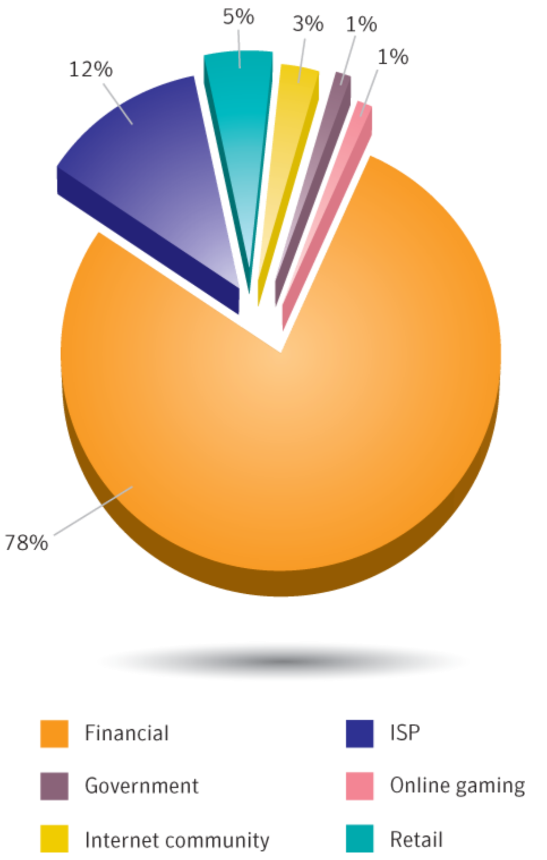
- Top advertised items on underground economy remain:
  - Credit card information
  - Bank accounts details
- Credit card dumps saw a marked increase in advertisements



Overall Rank			Percentage		
2009	2008	Item	2009	2008	Range of Prices
1	1	Credit card information	19%	32%	$0.85–$30
2	2	Bank account credentials	19%	19%	$15–$850
3	3	Email accounts	7%	5%	$1–$20
4	4	Email addresses	7%	5%	$1.70/MB–$15/MB
5	9	Shell scripts	6%	3%	$2–$5
6	6	Full identities	5%	4%	$0.70–$20
7	13	Credit card dumps	5%	2%	$4–$150
8	7	Mailers	4%	3%	$4–$10
9	8	Cash-out services	4%	3%	$0–$600 plus 50%–60%
10	12	Website administration credentials	4%	3%	$2–$30

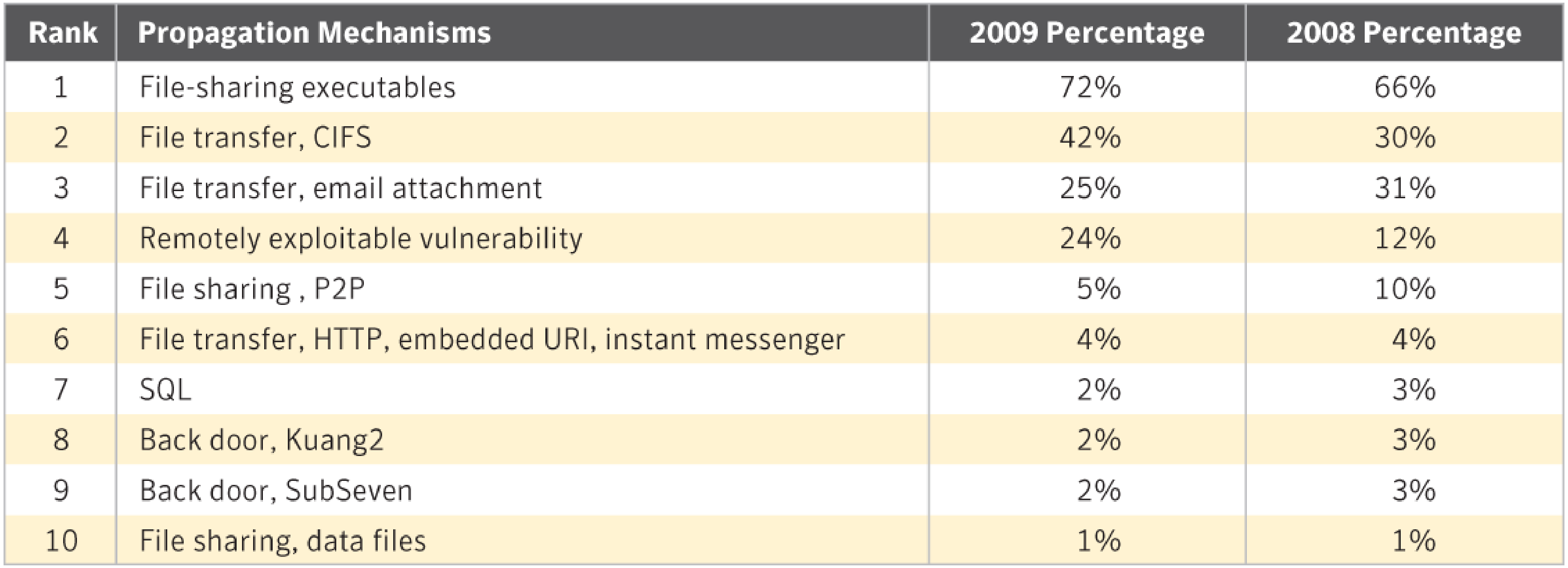
Threat Landscape: Underground Economy Still Strong

- Spammers and phishers continue to targeting financial services
- However, the social engineering reflects current economy
  - Messages incorporate themes of refinancing loans, consolidating debt, reducing credit card interest rates



Malicious Code Trends: How Infection Spreads

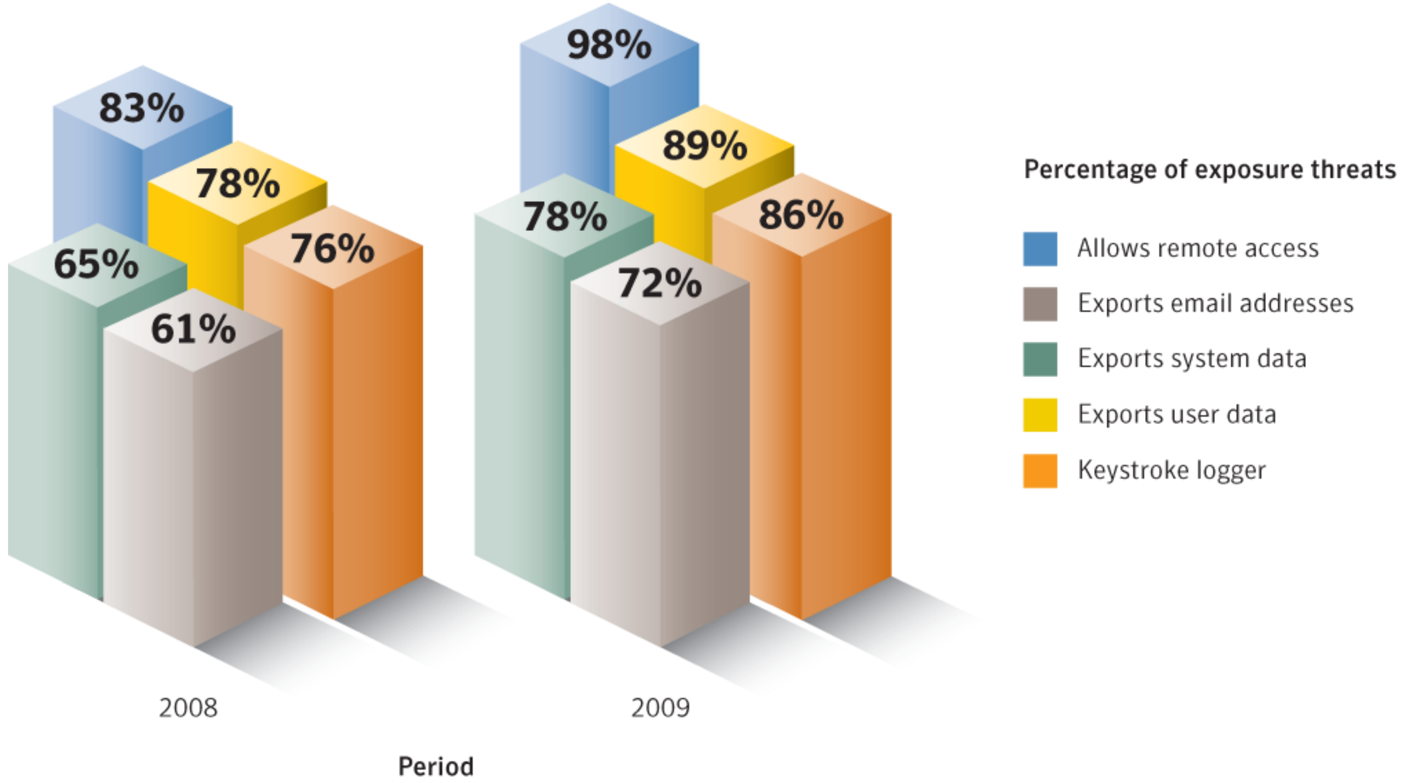
- 72% of malware propagation spreads via file-sharing executables
- Downadup (Conficker) big reason for increase in propagation
  - File-sharing executables were primary means of spreading



Rank	Propagation Mechanisms	2009 Percentage	2008 Percentage
1	File-sharing executables	72%	66%
2	File transfer, CIFS	42%	30%
3	File transfer, email attachment	25%	31%
4	Remotely exploitable vulnerability	24%	12%
5	File sharing , P2P	5%	10%
6	File transfer, HTTP, embedded URI, instant messenger	4%	4%
7	SQL	2%	3%
8	Back door, Kuang2	2%	3%
9	Back door, SubSeven	2%	3%
10	File sharing, data files	1%	1%

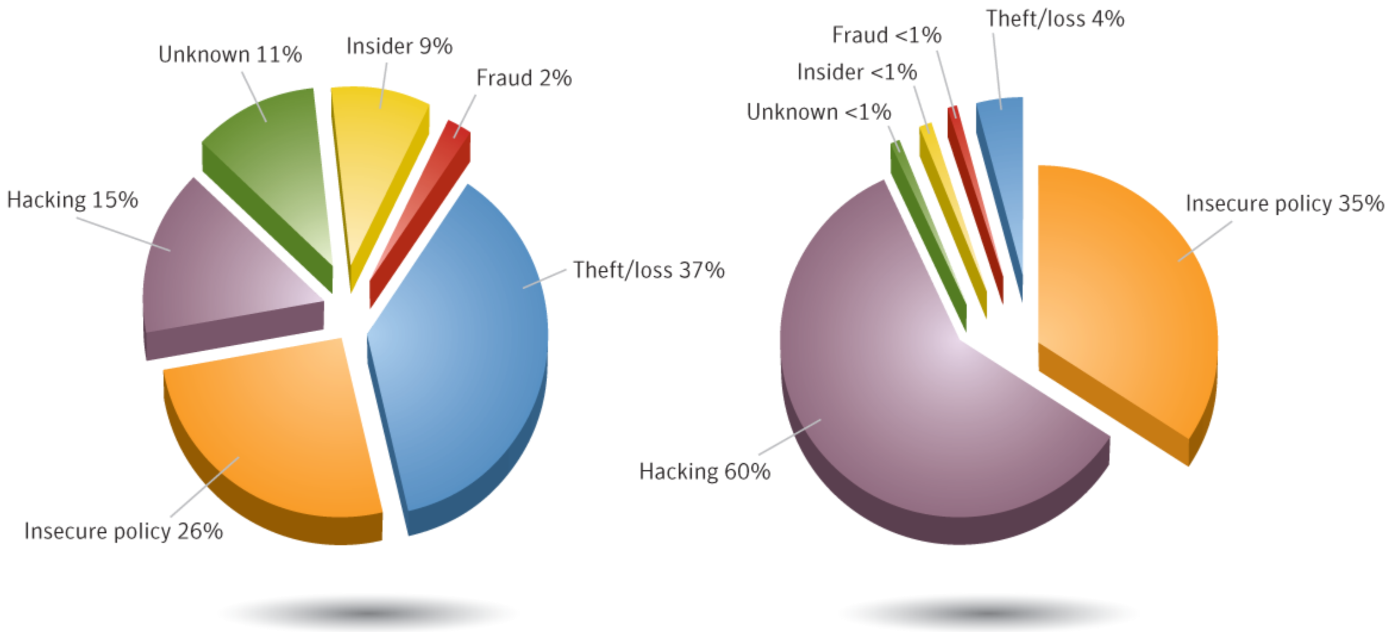
Threat Landscape: Attack Kits Lower Bar for ID Theft

- Almost ¾ of all threats contain more than one type of theft
- Attack kits are driving this trend



Threat Landscape: Targeted Attacks Focus on Enterprises

- Most data breaches are caused by theft or loss of a device, but …
- Hacking resulted in the greatest number of identities exposed



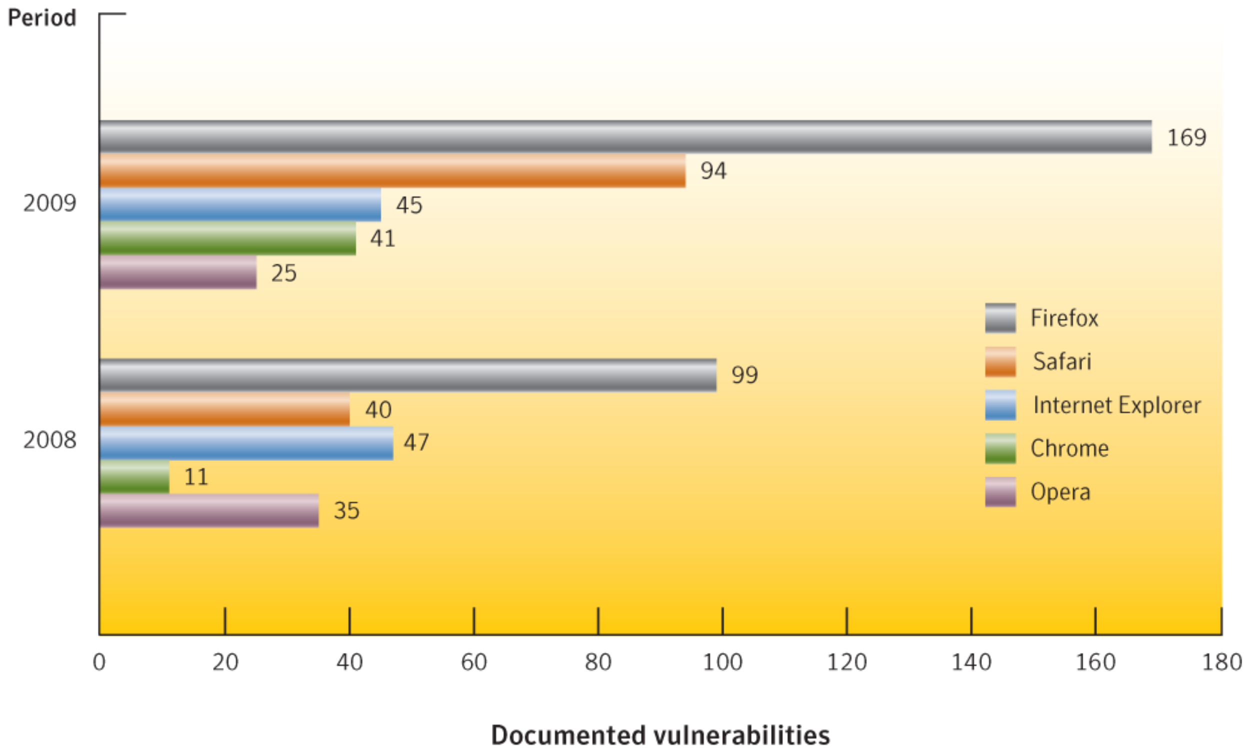
Data breaches

Identities exposed

ISTR XV: Key Facts & Figures

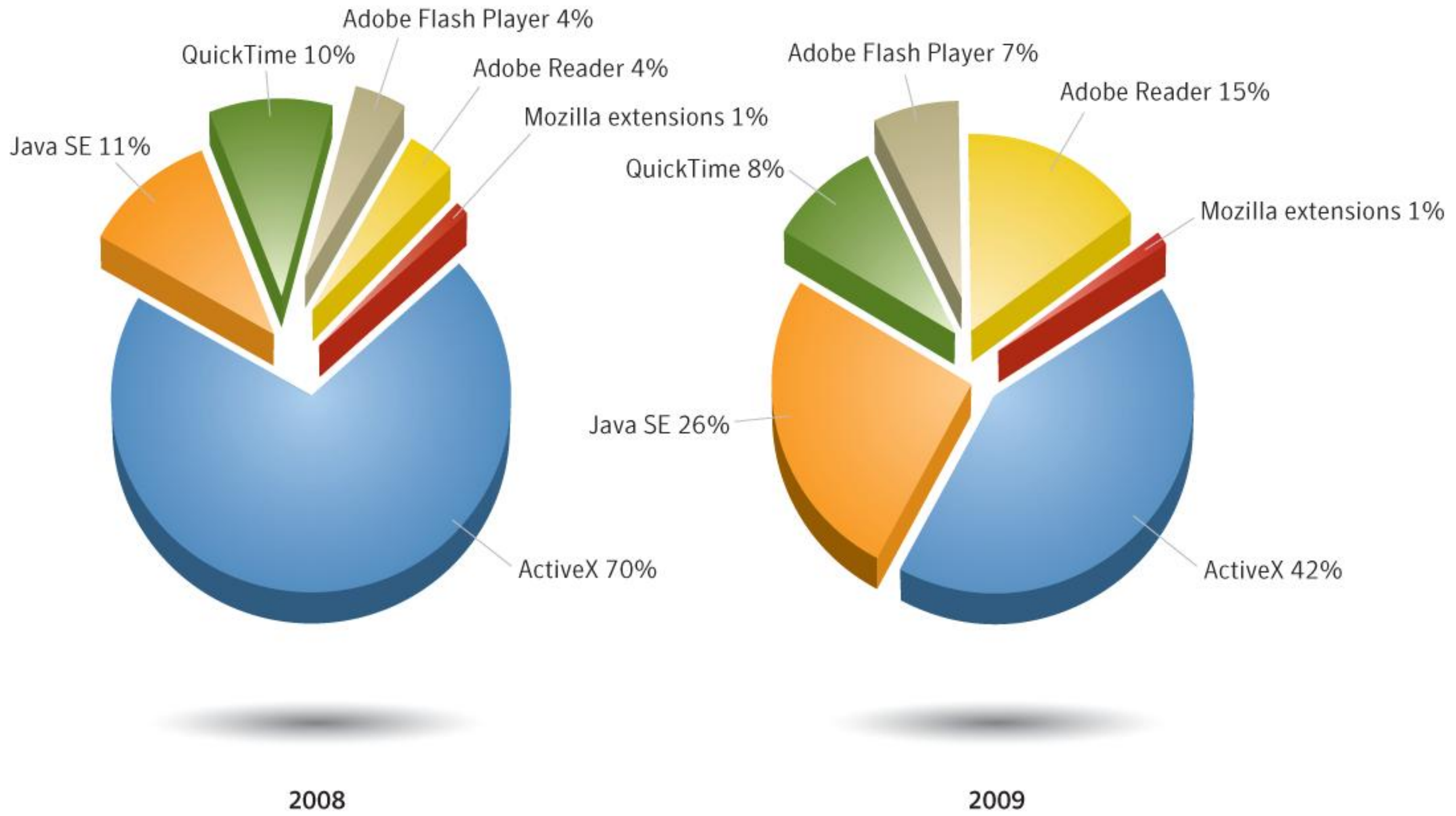
Vulnerability Trends: Web Browser Vulnerabilities

- Firefox had most, but shortest window of exposure
  - Cyber criminals attack popular browsers, not those with most vulnerabilities
- Of 374 Web browser vulnerabilities in 2009, 14% are unpatched



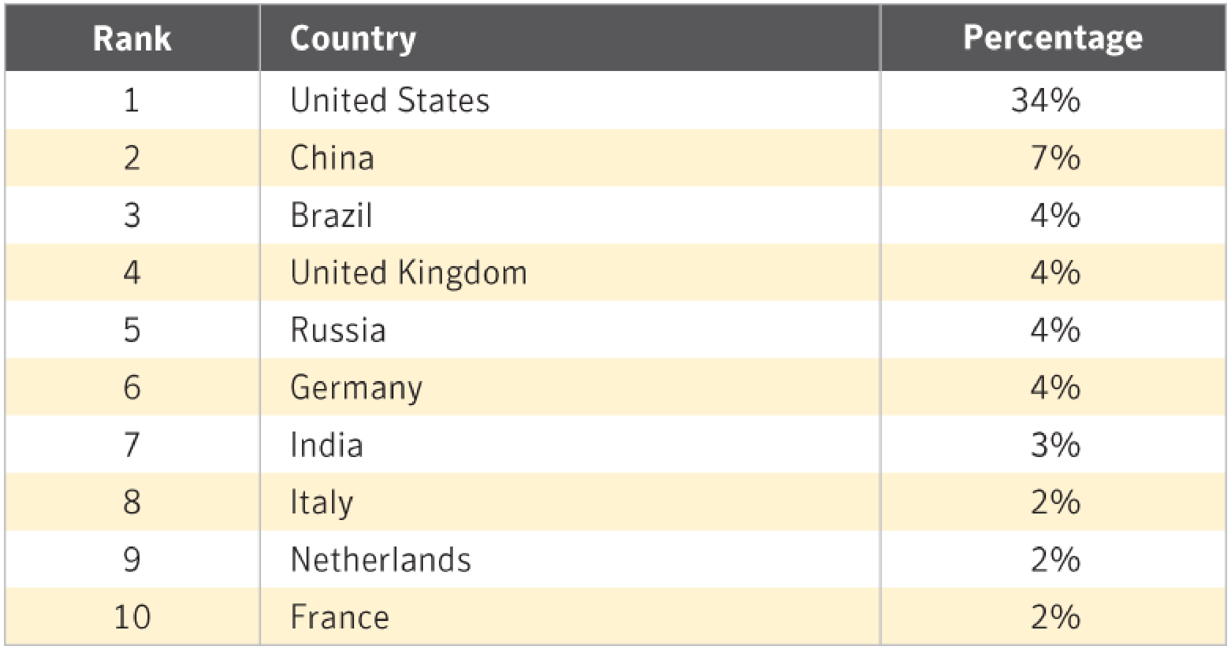
Vulnerability Trends: Web Browser Plug-In Vulnerabilities

- Web browser plug-in vulnerabilities exploited to install malware
- ActiveX had most, but Java and Acrobat grew significantly



Threat Landscape: Malicious Activity in Emerging Countries

- Brazil and India rank highly where Web-based attacks originate
- Web-based attacks may also be partly related to bot activity



Rank	Country	Percentage
1	United States	34%
2	China	7%
3	Brazil	4%
4	United Kingdom	4%
5	Russia	4%
6	Germany	4%
7	India	3%
8	Italy	2%
9	Netherlands	2%
10	France	2%

Countries of Origin for Web-based Attacks

Defending Against Threats

Preventive Security

- Policies
  - Top-down, clear, and enforceable
  - Include unstructured as well as structured data e.g., databases
  - Email, IM, blogging, text, etc.
  - Enforced
- Human Factors
  - Initial and periodic training
  - Ongoing reinforcement
- Technology
  - Easiest issue to address
  - Buying decisions bridge gap between policy and enforcement

Remedial Security

- Bad things will still happen
  - Accepted risk realization
  - Unknown or new threat exploitation
  - Zero-day attacks
- Deal with them by having:
  - Plans
    - In-place
    - Tested
  - People
    - Your staff and other state personnel
    - Outside resources
  - Partners
    - Management support
    - Technology partners who stand by their products

Thank you!

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.